ЕВРАЗИЙСКОЕ ПРОСТРАНСТВО: ИНТЕГРАЦИОННЫЕ ПРОЦЕССЫ И РЕГИОНАЛЬНЫЙ ОПЫТ УПРАВЛЕНИЯ

УДК 341
ББК 67.9

DOI 10.22394/1682-2358-2018-5-105-114

A.A. Kovalev, *Candidate of Science (Politics), Docent of the Public Administration Department, North-West Institute of Management, Branch of the Russian Presidential Academy of National Economy and Public Administration*

A.I. Balashov, *Doctor of Science (Economics), Head of the Public Administration Department, North-West Institute of Management, Branch of the Russian Presidential Academy of National Economy and Public Administration*

INTERNATIONAL LEGAL ASPECTS OF THE CYBERSECURITY POLICY OF SOME EUROPEAN COUNTRIES OF THE FORMER SOVIET BLOC

The international legal aspects of civil and power approaches to the issues of ensuring cyber security and the perception of possible threats and their sources based on the policies of the four countries of Eastern Europe and the Baltic States are analyzed. The classification of civil and power approaches to cybersecurity in the authorial study on extensive factual material can contribute to better understanding of cybersecurity as a phenomenon.

Key words and word-combinations: national security, information security, cybersecurity, information society, security strategy.

А.А. Ковалев, *кандидат политических наук, доцент кафедры государственного и муниципального управления Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте РФ (email: kovalev-aa@sziu.ranepa.ru)*

А.И. Балашов, *доктор экономических наук заведующий кафедрой государственного и муниципального управления Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте РФ (email: balashov-ai@sziu.ranepa.ru)*

МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ ПОЛИТИКИ КИБЕРБЕЗОПАСНОСТИ НЕКОТОРЫХ ЕВРОПЕЙСКИХ СТРАН БЫВШЕГО СОВЕТСКОГО БЛОКА

Аннотация. Анализируются международно-правовые аспекты гражданских и силовых подходов к вопросам обеспечения кибербезопасности и восприятию возможных угроз и их источников на основе политики четырех стран Восточной Европы и стран Балтии. Проведенная в исследовании на обширном фактическом материале классификация гражданских и силовых подходов к кибербезопасности может послужить лучшему пониманию кибербезопасности как явления.

Ключевые слова и словосочетания: национальная безопасность, информационная безопасность, кибербезопасность, информационное общество, стратегия безопасности.

Безопасность в современных условиях становится категорией, которой оперируют ученые многих гуманитарных и общественных дисциплин, в том числе социальной философии и политологии, философской антропологии и социологии, социальной психологии и международного права. Безопасность имеет огромное значение в глобальной политике и международных отношениях, ее различные аспекты регулируются на международно-правовом уровне.

На рубеже столетий появились новые угрозы как социальной, так и индивидуальной безопасности, возникшие вследствие бурного технического прогресса. Привычная человеку реальность впервые за всемирную историю дополнена реальностью виртуальной, или киберреальностью, ныне уже не являющейся исключительно метафизическим термином. Это не просто абстракция, введенная У. Гибсоном в рассказе 1982 г. «Сожжение Хром» и постоянно использующаяся в философии и компьютерных технологиях, а подлинное знамение нашего времени. Не случайно в США полным ходом идет процесс создания AFCYBER — специального военного формирования, цель которого станет ведение боевых оборонительных и наступательных действий в киберпространстве. Аналогичные шаги предпринимают многие европейские страны, а также Россия, оказавшаяся после распада СССР в кольце стран, некогда входивших в организацию Варшавского договора, а сегодня настроенных исключительно враждебно против бывшей метрополии. На заседании международного конгресса по кибербезопасности 6 июля 2018 г. Президент России В.В. Путин отметил, что «нейтрализация угроз и в целом обеспечение кибербезопасности — это государственная задача, и в ее решении необходимо объединение усилий правоохранительных органов, деловых кругов, общественных организаций и самих граждан» [1].

Некоторые государства рассматривают обеспечение кибербезопасности как гражданскую или экономическую задачу, но многие привлекают спецслужбы для создания или осуществления политики обеспечения кибербезопасности. Киберугрозы произвели революцию в представлении людей о безопасности, правилах и методах обеспечения национальной безопасности. Хотя всеобъемлющее определение киберугрозы представляется проблематичным, почти все государства согласны с тем, что угрозы и риски в киберпространстве должны быть учтены в их политике национальной безопасности. Проблематика эта исследуется довольно активно как в России [2—4], так и за рубежом [5; 6], но ее актуальность не ослабевает, ибо технологии развиваются настолько быстрыми темпами, что политики и юристы часто не успевают за меняющейся реальностью.

Применение основ теории безопасности позволит рассмотреть в данной публикации как гражданские, так и силовые подходы к вопросам обеспечения кибербезопасности и восприятию возможных угроз и их источников. Попытаемся исследовать политику кибербезопасности некоторых стран Восточной Европы и Балтии, которые ныне занимают в цивилизационном противостоянии ярко выраженную антироссийскую позицию. Существуют разнообразные доктрины, рассматривающие вопросы кибербезопасности. Парадигма национальной безопасности отражает традиционную роль государства в обеспе-

чении безопасности границ страны и соблюдении верховенства права [7]. Кибербезопасность ныне признается основополагающей для государственной военной и экономической безопасности, ее необходимость оправдывается традиционными аргументами национальной безопасности, основанными на защите государства [8].

В отличие от военного подхода к проблеме кибербезопасности, гражданский подход может быть проанализирован сквозь призму экономических императивов. Экономическая парадигма отражает растущее влияние созданной и привнесенной Интернетом реальности на экономическое благосостояние государств [7], с позиции которого существует два необходимых условия для осуществления национальной стратегии кибербезопасности: 1) поставщики услуг Интернета должны нести ответственность за ликвидацию зараженных вирусами компьютеров в своих системах; 2) организации и другие учреждения обязаны раскрывать данные об угрозах вторжения [9]. Экономическая парадигма относится к децентрализованному подходу между группой учреждений (организаций) и субъектов, отвечающих за управление кибербезопасностью. При таком подходе ответственность за принятие мер по защите систем в целом разделяют отдельные лица, поставщики услуг и государственные органы.

По словам Президента РФ В.В. Путина, в России реализуются конкретные меры, направленные на обеспечение безопасности в киберпространстве. Во-первых, вырабатываются новые комплексные решения по предупреждению и пресечению правонарушений против граждан в цифровой среде. Во-вторых, реализуются конкретные инициативы бизнес-сообщества по формированию системы автоматизированного обмена информацией об угрозах в цифровом пространстве. В-третьих, Российская Федерация стремится к тому, чтобы программное обеспечение и инфраструктура связи основывались на отечественных технологиях и решениях, прошедших соответствующую проверку и сертификацию. В-четвертых, при подготовке российских специалистов по противодействию киберпреступности целесообразно использовать передовой зарубежный опыт. Следует также развивать и совершенствовать систему международного обмена информацией о киберугрозах [1].

В ряду европейских стран, занимающихся реализацией политики кибербезопасности, интересен опыт Эстонии. Государством разработаны и приняты стратегические документы в этой сфере, созданы соответствующие институциональные структуры. Стратегическое планирование обеспечивает сплоченность всей архитектуры кибербезопасности. В 2008 г. Эстонская Республика одна из первых в мире приняла Национальную стратегию кибербезопасности [10], вписанную в рамки международного права. Эстония приступила к созданию условий, облегчающих использование информационно-коммуникационных технологий и разработку «умных решений» [11]. Министр иностранных дел Эстонии М. Кальюранд, выступая в 2016 г. в Брюсселе на конференции по управлению Интернетом в Европе «EuroDIG (European Dialogue on Internet Governance)», заявила о том, что «развитие ИКТ и кибербезопасность должны стать частью повседневной жизни людей, а не «люксовым товаром» [12].

С 2011 г. ответственность за координацию политики в области кибербезопасности Эстонии в целом перешла от Министерства обороны к Министерству по экономическим вопросам и коммуникациям. Совет по кибербезопасности Эстонии, являясь межведомственным органом, оказывает поддержку межведомственному сотрудничеству на стратегическом уровне и надзору за реализацией целей стратегии кибербезопасности страны. Министерство обороны является координационным органом для кибернетической обороны в области национальной обороны. С 2008 г. в составе сил обороны Эстонии находится Центр передового опыта НАТО по кибероборонe — Международная военная организация, которая сосредоточивает свои усилия на расширении возможностей кибернетической обороны НАТО и стран-партнеров. НАТО официально признало киберпространство операционной средой и таким образом приравняло существующие в нем угрозы к военным угрозам.

В 2017 г. в Таллинне был создан Объединенный центр передовых технологий по кибероборонe НАТО (NATO Cooperative Cyber Derence Centre of Excellence) — флагман европейской кибербезопасности. Центр получил аккредитацию НАТО, насчитывает 20 участников — 17 членов НАТО и три государства-партнера. В нем трудятся и военнослужащие, и гражданские лица, и представители Правительства Эстонской Республики. Работа Центра сфокусирована на трех основных направлениях: исследования, тренировки, обучение. Основная задача Центра — тренировка специалистов из разных стран, обеспечивающих безопасность в национальном киберпространстве. По словам директора Центра М. Майгре, «самыми опасными киберугрозами являются те, которые поддерживаются на государственном уровне» [13]. Центр ежегодно проводит крупнейшие в мире киберучения «Locked Shields» для экспертов в области киберзащиты. В 2017 г. в Таллинне прошли учения киберцентра НАТО под названием «Сомкнутые щиты» (Locked Shields 2017), вкоторых приняли участие около восьмисот специалистов из 25 стран в сферах информационных технологий, международного права, специальных служб, науки и СМИ. Сотрудниками Центра разрабатывается доктрина по киберзащите, то есть единый алгоритм действий в случае киберугроз. Планируется, что новая доктрина будет одобрена НАТО в 2019 г. Все это свидетельствует об активизации работы по виртуализации безопасности, включая военную.

В Латвийской Республике принята Стратегия кибербезопасности на период 2014—2018 гг. [14], в которой рассматриваются угрозы, связанные с безопасностью информационно-коммуникационных технологий в киберпространстве и дается прогноз по рискам киберопасности на будущее. В соответствии с Законом Латвии о безопасности информационных технологий [15] определяются основные требования по безопасности для государственных и муниципальных учреждений, поставщиков общедоступных электронных коммуникаций. Два документа отражают комплексный подход к защите безопасности в киберпространстве и национальной безопасности Латвии в целом. В рамках этой политики определены следующие направления деятельности: управление кибербезопасностью, правопорядок в киберпространстве и снижение уровня

киберпреступности, образование общества и исследовательская работа в этой сфере, международное сотрудничество.

При открытии в Риге в 2015 г. офиса Центра стратегических коммуникаций НАТО (Stratcom) Президент Латвии Р. Вейонис отметил, что «стратегические коммуникации играют ключевую роль в информационную эпоху» [16]. Президент Литвы Д. Грибаускайте подчеркнула, что латвийский офис является третьим центром в странах Балтии. В Эстонии функционирует центр НАТО по вопросам кибербезопасности, а в Литве — центр НАТО по вопросам энергетики. Министерство обороны Республики координирует участие Латвии в формировании международной политики в сфере кибербезопасности в соответствии с общим документом — «Обязательством по киберзащите» (Cyber Defence Pledge) [17]. Глава Ассоциации информационных и коммуникационных технологий Латвии С. Балиня высказывается о возможности привлечения латвийских хакеров к защите государства от кибератак: «Нам нужно собрать людей, которые имеют нужные навыки. Если появится необходимость, мы сможем мобилизовать людей» [18].

В Литовской Республике управление угрозами кибербезопасности прошло длительную эволюцию от создания учреждений, занимающихся вопросами кибербезопасности, до принятия закона о кибербезопасности [19]. По Глобальному индексу кибербезопасности, составленному Международным союзом электросвязи, Литва занимает 57-е место. В целом этот индекс отражает уровень киберзащищенности государств и усилия, которые прилагает конкретная страна для улучшения этого показателя. К слабым сторонам в литовской кибербезопасности можно отнести следующее: низкие стандарты в организациях, недостаточный уровень общественной осведомленности, отсутствие мер стимулирования и межгосударственных договоренностей [20].

В целях обеспечения безопасности киберпространства государства Правительство Литвы одобрило Программу развития электронной информационной безопасности на 2011—2019 гг. [21], целями которой заявлены: укрепление безопасности государственных информационных ресурсов; обеспечение эффективного функционирования критической информационной инфраструктуры; обеспечение кибербезопасности граждан Литвы и лиц, временно находящихся на территории страны. Эти цели были разработаны в соответствии с законодательством Литовской Республики по кибербезопасности, утвержденным в 2014 г. [19]. В соответствии с ним Министерству обороны предоставлено право координировать национальную политику по кибербезопасности, предполагается учреждение Национального центра кибербезопасности, создание Консультативного совета по кибербезопасности при Министерстве обороны.

Власти Литвы не раз изъявляли желание о взятии на себя роли лидера в вопросах кибербезопасности как в Европейском союзе, так и в сотрудничестве с США. В июне 2018 г. Сейм Литвы принял изменения к закону о кибербезопасности. В соответствии с поправками, подготовленными Минобороны Литвы, Правительство страны обязано принять Национальную стратегию за-

щиты от киберугроз в контексте развития международного сотрудничества и управления рисками на уровне Европейского союза.

В 2018 г. в Люксембурге Литва, Эстония, Хорватия, Румыния, Нидерланды, Испания подписали меморандум о создании кибернетических сил быстрого реагирования ЕС. Бельгия, Германия, Греция и Словения приняли решение присоединиться к проекту в качестве наблюдателей. Главная задача проекта состоит в том, чтобы создать в каждой стране команды быстрого реагирования из специалистов по вопросам кибербезопасности [22]. Это еще один шаг в рамках сотрудничества по вопросам кибербезопасности стран, которые некогда входили в зону Совета экономической взаимопомощи и Варшавского договора.

Кибербезопасность является частью системы национальной безопасности Польши. Впервые вопрос о кибербезопасности страны был поднят в 2007 г. в Стратегии национальной безопасности [23], где отмечалась прямая связь между кибербезопасностью и способностью государства функционировать должным образом. В 2014 г. Стратегия была обновлена, в ней подробно освещались вопросы, связанные с защитой киберпространства в Польше. В 2013 г. принят документ «Политика защиты киберпространства в Польше» [24]. В 2015 г. Бюро национальной безопасности Польши опубликовало Доктрину кибербезопасности [25], где намечены цели по повышению национальной безопасности в области киберпространства.

В Чешской Республике Национальная стратегия информационной безопасности, в которой поднимались вопросы регулирования безопасности в киберпространстве, впервые опубликована в 2005 г. В 2011 г. кибербезопасность была определена как одна из главных приоритетных задач Чешского правительства, а киберугрозы были приравнены к важнейшим угрозам безопасности, аналогичным региональным конфликтам, терроризму, оружию массового поражения. В 2015 г. утверждена Стратегия кибербезопасности Чешской Республики на период до 2020 г. [26], направленная на защиту систем информационно-коммуникационных технологий и минимизацию ущерба, вызванного киберпреступлениями. В 2015 г. Правительство Чехии утвердило обновленную Стратегию национальной безопасности [27], где подчеркиваются нарастающие проблемы Чешской Республики и других членов НАТО и Европейского союза, порожденные изменениями в обстановке безопасности, ухудшением ситуации на европейской периферии. Речь идет об угрозах и рисках ослабления европейской безопасности, новых аспектах терроризма и насущных проблемах кибербезопасности.

В 2017 г. в Чешской Республике создан Национальный офис по кибербезопасности и информации (NUKIB) — структура, в функции которой входит решение проблем кибербезопасности, поддержка государственных учреждений и предприятий в случае кибератак, профилактика преступлений в киберпространстве, обеспечение безопасности информационной инфраструктуры.

С 2017 г. в Чехии функционирует Центр борьбы с терроризмом и гибридными угрозами. Решение о его создании было принято после аудита национальной безопасности. Центр подчинен Министерству внутренних дел Чехии,

его основные задачи — наблюдение за подозрительными публикациями в Интернете, разоблачение «фейковых новостей» с целью воспрепятствования их широкому распространению, борьба против «пропаганды внешних сил».

Словацкая Республика впервые разработала концептуальную основу своей кибербезопасности в 2008 г., приняв Национальную стратегию информационной безопасности Словацкой Республики на 2009—2013 гг. [28]. В 2015 г. приняты два документа: Концепция кибербезопасности Словацкой Республики на 2015—2020 гг.» [29] и План действий по Концепции кибербезопасности Словацкой Республики на 2015—2020 гг. [30]. Служба национальной безопасности Словакии занимается вопросами управления секретной информацией; Министерство обороны непосредственной роли в управлении национальной кибербезопасностью не играет.

В Национальной стратегии кибербезопасности Венгрии, принятой в 2013 г., четко прописано, что защита суверенитета страны в киберпространстве является национальным интересом [31]. Осознавая тот факт, что угрозы и нападения, возникающие в киберпространстве, могут перейти грань, требующую сотрудничества со странами НАТО, Венгрия считает крайне важным, чтобы кибербезопасность стала вопросом коллективной обороны в соответствии со ст. 5 основополагающего договора НАТО. Это важный шаг на пути международно-правового обеспечения кибербезопасности. Следует отметить, что киберугрозы также являются приоритетными в Стратегии национальной безопасности Венгрии, принятой в 2012 г. [32].

Итак, обзор национальных стратегий кибербезопасности в семи европейских странах бывшего советского блока показал, что их стратегии кибербезопасности становятся комплексными и всеобъемлющими. Эти стратегии охватывают экономические, социальные, международно-правовые, правоохранительные, военные аспекты кибербезопасности. В рамках сотрудничества по линии ОБСЕ рассмотренные государства работают над мерами укрепления доверия с целью снижения рисков возникновения конфликтов вследствие пользования информационно-коммуникационными технологиями.

Все семь государств признают взаимосвязь между сферой кибер- и национальной безопасностью и осознают, что проблемы кибербезопасности, такие как разрушение системы информационно-коммуникационных технологий или критической инфраструктуры, могут нанести ущерб национальной безопасности и действенному функционированию экономики государства. Страны, стремящиеся к секьюритизации своего киберпространства, с большей вероятностью будут уделять первоочередное внимание защите критической инфраструктуры как ключевого условия национальной безопасности.

Существующая архитектура киберпространства в европейских государствах облегчает анонимность и препятствует возможности отслеживать источники кибератак, что является дополнительным фактором отсутствия безопасности. Страны, активно защищающие свое киберпространство, подчеркивают политическую мотивацию кибератак и внешних киберугроз. Такое отношение диктует силовой подход к управлению кибербезопасностью как наибо-

лее эффективный. Сосредоточение внимания главным образом на внутренних угрозах кибербезопасности означает, что основным объектом безопасности выступает экономическая сфера.

Восприятие киберугроз тесно связано с источниками воспринимаемых угроз. Чем больше секьюритизируется взгляд на киберугрозы, тем точнее выявляется источник угрозы. Эстония, Польша, Литва и Латвия проводят различие между внешними и внутренними субъектами киберпространства. Примечательно, что почти все проанализированные страны проводят различие между внутренними и внешними источниками киберугроз в своих стратегических документах. Однако страны, ориентированные на гражданский подход, не стремятся к дальнейшей проработке этого различия и сосредоточивают свое внимание главным образом на внутренних источниках угрозы как наиболее распространенных и вероятных в условиях их безопасности.

Каждая из рассмотренных стран имеет свою стратегию кибербезопасности и соответствующие законы для решения проблем кибербезопасности. Польша, Эстония, Литва и в некоторой степени Латвия милитаризируют вопросы кибербезопасности. Эта тенденция поднимает кибербезопасность до уровня национальной безопасности и фокусируется на защите государственных ресурсов информационно-коммуникационных технологий. Польша, Эстония и Литва склонны идентифицировать проблемы кибербезопасности как угрозы нормальному функционированию государства и выявлять нападения со стороны иностранных государств как наиболее опасные источники таких угроз. В этих государствах ответственность за нейтрализацию киберугроз передается силовым учреждениям.

Вторая категория секьюритизационной сферы относится к решению угроз, связанных с возможной криминализацией кибербезопасности. Чехия, Словакия и Венгрия полагаются на гражданский подход к обеспечению своей кибербезопасности. Их объекты безопасности разрознены и в основном связаны с надлежащим функционированием экономической системы государства и частной собственности. В результате страны с преобладающим гражданским подходом в основном заняты борьбой с преступной деятельностью, проводимой в киберпространстве, и описывают вопросы кибербезопасности как «риски». Потенциальные источники таких рисков также фрагментированы и включают не только внешних международных субъектов, но и внутренних субъектов, таких как хакеры, хактивисты, преступные организации. Гражданским учреждениям в Чехии, Словакии и Венгрии поручено следить за рисками кибербезопасности и координировать реакцию государства на киберинциденты.

Проведенная классификация подходов к кибербезопасности может послужить лучшему пониманию кибербезопасности как явления, что, в свою очередь, способствует снятию ряда проблем на пути сотрудничества между государствами, занимающимися вопросами кибербезопасности на международном уровне. Более того, идентификация различных подходов к кибербезопасности способствует объяснению действий конкретного государства в киберпространстве. Понимание различий государств в существующем восприятии киберугроз, объектов безопасности и потенциальных противников

представляет собой предпосылки для обсуждения так называемых кибериденти-чностей государств и негосударственных субъектов — полезного теоретического инструмента для анализа потенциальных киберконфликтов и моделей сотрудничества в дальнейших научных исследованиях.

Библиографический список

1. Пленарное заседание Международного конгресса по кибербезопасности // Официальный сайт Президента Российской Федерации. URL: http://kremlin.ru/events/president/news/57957

2. От информационной безопасности к кибербезопасности: опыт научно-исследовательских работ и подготовки кадров в Санкт-Петербургском политехническом университете Петра Великого. СПб., 2017.

3. Проблемы кибербезопасности информационного общества / под ред. Д.С. Черешкина. М., 2006.

4. Словарь-справочник терминов в области кибербезопасности. М., 2014.

5. Cyber warfare and cyber terrorism / L.J. Janczewski, A.M. Colarik. N.Y., 2008.

6. Cyberterrorism / ed. by Alan O'Day. Burlington: Aldershot Hants, 2004.

7. *Newmeyer K.P*. Elements of national cybersecurity strategy for developing nations // National Cybersecurity Institute Journal. 2015. № 1(3). P. 9–19.

8. *Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В*. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (ч. 1) // Вопросы безопасности. URL: https://cyberleninka.ru/article/v/kiberbezopasnost-kak-osnovnoy-faktor-natsionalnoy-i-mezhdunarodnoy-bezopasnosti-hh-veka-chast-1

9. *Moore T*. Introducing the economics of cybersecurity: Principles and policy options. URL: https://www.nap.edu/read/12997/chapter/3

10. Стратегия кибербезопасности Эстонской Республики. URL: https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf

11. Основы политики безопасности Эстонской Республики. URL: http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/julgeolekupoliitika_alused_2010.pdf

12. Закон Литовской Республики о кибербезопасности. URL: https://ccdcoe.org/sites/default/files/strategy/LTU_CSAct_lt.pdf

13. Юри Ратас в Центре киберзащиты НАТО: наши идеалы нужно оберегать // Новостное агентство Sputnik. URL: https://ru.sputnik-news.ee/news/20180627/11360194/ratas-tallinn-tsentr-kiberzashita-nato-idealy-nuzhno-oberegatj.html

14. О руководящих принципах Стратегии кибербезопасности Латвийской Республики на 2014–2018 гг. URL: https://likumi.lv/doc.php?id=263912

15. Law On the Security of Information Technologies. URL: http://www.dvi.gov.lv/en/legal-acts/law-on-the-security-of-information-technologies/

16. В Латвии открылся новый офис Центра стратегических коммуникаций НАТО // Информационное телеграфное агентство России. URL: https://tass.ru/mezhdunarodnaya-panorama/2198715

17. Обязательство по киберзащите // Официальный сайт НАТО. URL: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

18. Киберземессардзе хочет мобилизовать латвийских хакеров // Новостное агентство Sputnik. URL: https://ru.sputniknewslv.com/Latvia/20170207/3841202/kiber-opolchenie-haker-latvija-zemessardze-ataka.html

19. Закон Литовской Республики о кибербезопасности. URL: https://ccdcoe.org/sites/default/files/strategy/LTU_CSAct_lt.pdf

20. Основы политики безопасности Эстонской Республики. URL: http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/julgeolekupoliitika_alused_2010.pdf

21. Об утверждении программы развития электронной информационной безопасности Литовской Республики на 2011–2019 гг. URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.403385

22. ЕС создаст европейские силы быстрого реагирования // Новостное агентство Sputnik. URL: https://sputniknews.com/europe/201806251065747571-eu-cyber-rapid-reaction-forces/

23. Стратегия национальной безопасности Республики Польша (в ред. от 2014 г.). URL: https://www.files.ethz.ch/isn/156796/Poland-2007-eng.pdf

24. Политика защиты киберпространства в Республике Польша. URL: http://www.cert.gov.pl/download/3/162/PolitykaOchronyCyberprzestrzeniRP148x210wersjaang.pdf

25. Доктрина кибербезопасности Республики Польша. URL: http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf

26. Стратегия кибербезопасности Чешской Республики на период с 2015 по 2020 г. URL: https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_cz.pdf

27. Стратегия безопасности Чешской Республики. URL: https://www.mzv.cz/file/1386521/Bezpecnostni_strategie_2015.pdf

28. Стратегия национальной безопасности Словацкой Республики. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncssmap/Slovakia_National_Strategy_for_ISEC.pdf

29. Концепция кибербезопасности Словацкой Республики на 2015–2020 гг. URL: https://ccdcoe.org/sites/default/files/strategy/SVK_NCSS.pdf

30. План действий по реализации Концепции кибербезопасности Словацкой Республики на 215–2020 гг. URL: https://lt.justice.gov.sk/Attachment/vlastny_material_rtf.pdf

31. Национальная стратегия кибербезопасности Венгрии. URL: https://iccwbo.org/content/uploads/sites/3/2016/11/Hungary-National-Cyber-Security-Strategy-1.pdf